Dkt. 0655/64514

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of : Doron ELGRESSY et al.

Serial No. : Not Yet Assigned

Date Filed : Continuation of PCT International Application No. PCT/IL99/00539, filed October 13, 1999

For : METHOD AND SYSTEM FOR THE PREVENTION OF UNDESIRABLE ACTIVITIES OF EXECUTABLE OBJECTS

1185 Avenue of the Americas
New York, N.Y. 10036

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to examination on the merits, please the above-identified application as follows:

IN THE SPECIFICATION:

Please insert before the first line of page one of the specification:

--This application is a continuation of PCT International application No. PCT/IL99/00539, filed October 13, 1999, designating the United States of America--.

I hereby certify that this paper is being deposited this date with the U.S Postal Service as first class mail addressed to Assistant Commissioner for Patents, Washington, D.C. 20231.

March 19, 2001

Richard F. Jaworski — Date
Reg. No. 33,515

IN THE CLAIMS:

Please cancel claim 17 without prejudice.

Please amend claims 1-16 as follows:

1. (Amended) A method of preventing undesirable activities of Executable Objects via an application, comprising denying to the same application, or one or more of its threads, access to a secured resource if said application, or one or more of its threads, has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource, and denying said application, or one or more of its threads, Internet behavior if, at a time access is sought to the Internet, said application, or one or more of its threads is accessing a secured resource.

2. (Amended) A method according to claim 1, further comprising recording in a memory events representative of Internet behavior, keeping a record of all secured resources that are to be kept secured and when an application that has previously exhibited Internet behavior attempts to access one such secured resource, denying access to said secured resource, unless:

a) At least a predetermined period of time has passed since a last Internet behavior; or

b) Said application, or one or more of its threads, has performed at least a predetermined number of operations after exhibiting Internet behavior; or

c) Another preset condition has been fulfilled.

3. (Amended) A method according to claim 2, wherein the preset condition comprises an exercise of control over execution of downloadables received during Internet behavior, to ensure that no unexecuted downloadable may access the secured resource.

4. (Amended) A method according to claim 2, wherein the present condition comprises an analysis of downloadables to ascertain the downloadables are harmless.

5. (Amended) A method according to claim 1, wherein Internet behavior is denied by disabling a network connection creation.

6. (Amended) A method according to claim 1, wherein Internet behavior is denied by disabling specific protocols.

7. (Amended) A method according to claim 6, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

8. (Amended) A method according to claim 1, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

9. (Amended) A method according to claim 5, wherein access to trusted sites is not denied.

10. (Amended) A method according to claim 1, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

11. (Amended) A method according to claim 1, wherein all sub-threads of a thread that is denied access to a secured resource are also denied access to secured resources.

12. (Amended) A method according to claim 1, wherein all sub-threads of a thread that is denied Internet behavior are also denied Internet behavior.

13. (Amended) Apparatus for preventing undesirable activities of Executable Objects via an application, comprising a memory for storing a record of Internet behavior of a plurality of applications, and means for denying to an application access to a secured resource if the application has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

14. (Amended) Apparatus for preventing undesirable activities of Executable Objects via an application, comprising a memory of storing a record of Internet behavior of a plurality of applications, and means for denying an application, or one or more of its threads, Internet behavior if, at a time access is sought, said application, or one or more of its threads, is accessing a secured resource.

15. (Amended) A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet, or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying to an application access to a secured resource if the application has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

16. (Amended) A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying an application, or one or more of its threads, Internet behavior if, at a time Internet behavior is exhibited, said application, or one or more of its threads, is accessing a secured resource.

Please add claims 18-33 as follows

18. (New) A method according to claim 2, wherein Internet behavior is denied by disabling a network connection creation.

19. (New) A method according to claim 3, wherein Internet behavior is denied by disabling a network connection creation.

20. (New) A method according to claim 4, wherein Internet behavior is denied by disabling a network connection creation.

21. (New) A method according to claim 2, wherein Internet behavior is denied by disabling specific protocols.

22. (New) A method according to claim 3, wherein Internet behavior is denied by disabling specific protocols.

23. (New) A method according to claim 4, wherein Internet behavior is denied by disabling specific protocols.

24. (New) A method according to claim 21 wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

25. (New) A method according to claim 22, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

26. (New) A method according to claim 23, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

27. (New) A method according to claim 2, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

28. (New) A method according to claim 3, wherein Internet behavior is denied by disabling transfer of executable objects in communication protocols.

29. (New) A method according to claim 4, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

30. (New) A method according to claim 1, wherein access to trusted sites is not denied.

31. (New) A method according to claim 2, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

32. (New) A method according to claim 3, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

33. (New) A method according to claim 4, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

REMARKS

Claims 1-16 have been amended to correct formal matters only. The scope of the claims has not been changed. Claim 17 has been cancelled without prejudice and claims 18-33 have been added. Claims 1-16 and 18-33 are in the case, wit claims 1 and 13-16 being in independent form.

The Office is hereby authorized to charge any additional fees which may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition, and the Commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this amendment and allowance of this application are respectfully requested.

Respectfully submitted,

RICHARD F. JAWORSKI
Reg. No. 33,515
Attorney for Applicants
Cooper & Dunham LLP
Tel.: (212) 278-0400

VERSION WITH MARKINGS TO SHOW CHANGES IN THE SPECIFICATION

Please insert before the first line of page one of the specification:

--This application is a continuation of PCT International application No. PCT/IL99/00539, filed October 13, 1999, designating the United States of America--.

VERSION WITH MARKINGS TO SHOW CHANGES IN THE CLAIMS

1. (Amended) A method of preventing undesirable activities of Executable Objects via an application, comprising denying to the same application, or one or more of its threads, access to a secured resource if [it] said application, or one or more of its threads, has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource, and denying said application, or one or more of its threads, Internet behavior if, at [the] a time access is sought to the Internet, [it] said application, or one or more of its threads is accessing a secured resource.

2. (Amended) A method according to claim 1, further comprising recording in a memory events representative of Internet behavior, keeping a record of all secured resources that are to be kept secured and when an application that has previously exhibited Internet behavior attempts to access one such secured resource, denying access to said secured resource, unless:

a) At least a predetermined period of time has passed since [the] a last Internet behavior; or

b) [It] Said application, or one or more of its threads, has performed at least a predetermined number of operations after exhibiting Internet behavior; or

c) Another preset condition has been fulfilled.

3. (Amended) A method according to claim 2, wherein the preset condition comprises [the] an exercise of control over [the] execution of downloadables received during Internet behavior, to ensure that no unexecuted downloadable may access the secured resource.

4. (Amended) A method according to claim 2, wherein the present condition comprises [the] an analysis of [the] downloadables to ascertain [that there] the downloadables are harmless.

5. (Amended) A method according to [any one of claims 1 to 4] claim 1, wherein Internet behavior is [blocked] denied by disabling [the] a network connection creation.

6. (Amended) A method according to [any one of claims 1 to 4] claim 1, wherein Internet behavior is [blocked] denied by disabling specific protocols.

7. (Amended) A method according to claim 6, wherein the specific protocols comprise HTTP, FTP, SMTP, or [the] like communication protocol.

8. (Amended) A method according to [any one of claims 1 to 4] claim 1, wherein Internet behavior is [blocked] denied by disabling [the] a transfer of [Eos] executable objects in [the] communication protocols.

9. (Amended) A method according to [any one of claims 5 to 8] claim 5, wherein [the] access to trusted sites is not [disabled] denied.

10. (Amended) A method according to [any one of claims 1 to 4] claim 1, wherein access to a secured resource is [blocked] denied by disabling a thread using a specific system service that is used to access the secured resource.

11. (Amended) A method according to [any one of claims 1 to 10] claim 1, wherein all sub-threads of a thread that is denied access to a secured resource are also denied access to secured resources.

12. (Amended) A method according to [any one of claims 1 to 10] claim 1, wherein all sub-threads of a thread that is denied Internet behavior are also denied Internet behavior.

13. (Amended) Apparatus for preventing undesirable activities of Executable Objects via an application, comprising a memory for storing a record of Internet behavior of a plurality of applications, and means for denying to [the same] an application access to a secured resource if [it] the application has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

14. (Amended) Apparatus for preventing undesirable activities of Executable Objects via an application, comprising a memory of storing a record of Internet behavior of a plurality of

applications, and means for denying [said] an application, or one or more of its threads, Internet behavior if, at [the] a time access is sought, [it] said application, or one or more of its threads, is accessing a secured resource.

15. (Amended) A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet, or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying to [the same] an application access to a secured resource if [it] the application has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

16. (Amended) A system for preventing undesirable activities of Executable Objects via an application, comprising a computer on which one or more applications are to run, said computer being connectable to the Internet or Intranet or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said plurality of applications, and means for denying [said] an application, or one or more of its threads, Internet behavior if, at [the] a time Internet behavior is exhibited, [it] said application, or one or more of its threads, is accessing a secured resource.

Please add claims 18-33 as follows

18. (New) A method according to claim 2, wherein Internet behavior is denied by disabling a network connection creation.

19. (New) A method according to claim 3, wherein Internet behavior is denied by disabling a network connection creation.

20. (New) A method according to claim 4, wherein Internet behavior is denied by disabling a network connection creation.

21. (New) A method according to claim 2, wherein Internet behavior is denied by disabling specific protocols.

22. (New) A method according to claim 3, wherein Internet behavior is denied by disabling specific protocols.

23. (New) A method according to claim 4, wherein Internet behavior is denied by disabling specific protocols.

24. (New) A method according to claim 21 wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

25. (New) A method according to claim 22, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

26. (New) A method according to claim 23, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

27. (New) A method according to claim 2, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

28. (New) A method according to claim 3, wherein Internet behavior is denied by disabling transfer of executable objects in communication protocols.

29. (New) A method according to claim 4, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

30. (New) A method according to claim 1, wherein access to trusted sites is not denied.

31. (New) A method according to claim 2, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

32. (New) A method according to claim 3, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

33. (New) A method according to claim 4, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.